REMARKS

In the Office Action, Claims 1-35 were examined and stand rejected. In response, Claims 1, 6, 11, 21, 26 and 31 are amended, no claims are cancelled and no claims are added. Applicant respectfully requests reconsideration of pending Claims 1-35 in view of the following remarks.

I. Claims Rejected Under 35 U.S.C. §101

Claims 1-20 and 31-35 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

Claims 6 and 31 are amended to recite an article of manufacturer including a machine readable storage medium encoded with instructions which may be used to program a system to perform a method, comprising. In view of Applicant's amendment to Claims 6 and 31, we submit that such claims are directed towards statutory subject matter.

Regarding Claim 1, the useful concrete and tangible result provided is a decrypted data block, which is decrypted according to a keystream that is generated within a predetermined time required to read the encrypted data block from the memory. Per the "Clarification of Interim Guidelines for Examination of Patent Applications for Subject Matter Eligibility," we submit that the ability to regenerate a keystream within a predetermined time required to read the encrypted data block from a memory enables secure storage of data within a memory where the reading and decryption of such data does not exacerbate a memory read latency for access to such memory.

Hence, we submit that Claim 1 provides an improved method for enabling secure storage of data where read back of such encrypted data is performed within a predetermined time required for reading of the encrypted data block and therefore does not further exacerbate a memory read latency.

Regarding Claim 11, Claim 11 recites:

> computing a keystream from the initialization vector and a secret key using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of a memory.

We submit that Claim 11 provides a useful concrete and tangible result of the form of an encrypted data block that is stored within memory where a number of rounds required to compute a keystream that encrypts the data block is reduced to match a memory read latency to

provide secure data storage without exacerbating the memory read latency that is prevalent between processors and memory.

In view of the above, Applicant respectfully submit that Claims 1-20 and 31-35 recite patentable subject matter according to 35 U.S.C. §101. Therefore, we request that the Examiner withdraw the 35 U.S.C. §101 rejection of Claims 1-20 and 31-35.

II. Claims Rejected Under 35 U.S.C. §102(b)

The Examiner rejects Claims 1-2, 5-7, 10-15, 17-32 and 34-35 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,809,148 issued to Doberstein et al. ("Doberstein"). Applicant respectfully traverses this rejection.

Claim 1 recites:

> reading an encrypted data block from memory;
> regenerating, within a time required to read the encrypted data block from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block; and
> once reading of the encrypted data block is complete, decrypting the encrypted data block according to the generated keystream.

Doberstein is generally directed to a method for decrypting retransmitted, encrypted data, where the retransmission does not include an entire message. (See col. 3, lines 4-6.) In contrast with Claim 1, Doberstein does not disclose or suggest reading an encrypted data block from memory, much less the regeneration of a keystream used to encrypt the data block within a predetermined time required to read the encrypted data block from the memory, as in Claim 1. Doberstein does disclose the ability to decrypt selected parts of a message without unnecessary delays or redundant work such as waiting retransmission of an entire message or redecrypting data in order to decrypt the entire message (see col. 3, lines 16-20), however, that is something completely different from regenerating a keystream used to encrypt a data block within a predetermined time required to read the encrypted data block from a memory, as in Claim 1.

According to the Examiner, the receipt of the requested retransmission of data discloses reading an encrypted data block from memory, as in Claim 1, while the use of a keystream that is either pulled from storage or regenerated from data to enable decryption of data without having to receive an entire message discloses the regenerating of a keystream, as in Claim 1. (See page 3, last ¶ of the Office Action mailed 4/05/07.) However, for at least the reasons indicated above,

we submit that the passages referred to by the Examiner describe the use of a keystream for decrypting retransmitted blocks that were received in error. Apposite to Claim 1, Doberstein teaches that a keystream is not regenerated for retransmitted data blocks until each of such retransmitted blocks are received without error. (See, col. 3, lines 13-16.)

Hence, neither the sections referred to by the Examiner nor any other disclosure in Doberstein discloses or suggests the reading of an encrypted data block from memory, much less the regeneration of the keystream used to encrypt the data block within a predetermined time required to read the encrypted data block from memory, as in Claim 1.

For each of the above reasons, therefore, Claim 1 and all claims which depend from Claim 1 are patentable over the cited art. Therefore, Applicants respectfully request that the Examiner reconsider and withdraw the §102(b) rejection of Claims 1-2 and 5.

Each of Applicants' other independent claims recite similar features to the novel claim features of Claim 1, as discussed above, and are therefore also patentable over the cited references. In view of the above, Applicants respectfully request that the Examiner withdraw the §102(b) rejection of Claims 6-7, 10-15, 17-32 and 34-35.

III. Claims Rejected Under 35 U.S.C. §103

The Examiner has rejected Claims 3 and 8 under 35 U.S.C. §103(a) as being unpatentable over Doberstein in view of Lynn.

In view of the above remarks, a specific discussion of the dependent claims is considered to be unnecessary. Therefore, Applicants' silence regarding any dependent claim is not to be interpreted as an agreement with, or acquiescence to, the rejection of such claim or as waiving any argument regarding that claim.

IV. Allowable Subject Matter

The Examiner has indicated that Claims 4, 9, 16 and 33 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form, including all of the limitations of the base claim and any intervening claims.

Regarding Claims 4, 9, 16 and 33, Claims 4, 9, 16 and 33 are also novel based on their dependency from Claims 1, 6, 11 and 31, respectively, for at least the reasons indicated above. Accordingly, Applicant respectfully requests that the Examiner allow Claims 4, 9, 16 and 33, based on their dependency from Claims 5, 6, 11 and 31, respectively.

CONCLUSION

In view of the foregoing, it is submitted that Claims 1-35 patentably define the subject invention over the cited references of record, and are in condition for allowance and such action is earnestly solicited at the earliest possible date. If the Examiner believes a telephone conference would be useful in moving the case forward, he is encouraged to contact the undersigned at (310) 207-3800.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§1.16 or 1.17, particularly, extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: 6/12/07

By: _____
Joseph Lutz, Reg. No. 43,765

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
Telephone (310) 207-3800
Facsimile (310) 820-5988

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below to the United States Patent and Trademark Office.

_____ 6/12/07
Elaine Kwak Date